- обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (подписан в г. Страсбург 16.09.1963), «Протоколом № 7» (подписан в г. Страсбург 22.11.1984)) // СЗ РФ. 2001. № 2. Ст. 163.
5. Постановление ЕСПЧ от 12.01.2016 «Дело «Сабо и Виши (SzaboandVissy) против Венгрии» (жалоба № 37138/14) // Прецеденты Европейского Суда по правам человека. 2016. № 7(31).
 6. «Типовой кодекс этики и служебного поведения государственных служащих Российской Федерации и муниципальных служащих» (одобрен решением президиума Совета при Президенте РФ по противодействию коррупции от 23 декабря 2010 г. (протокол № 21)) // Официальные документы в образовании. № 36. Декабрь. 2011.
 7. «Типовой кодекс этики и служебного поведения государственных и муниципальных служащих» Типовой кодекс этики и служебного поведения государственных служащих Российской Федерации и муниципальных служащих одобрен решением президиума Совета при Президенте Российской Федерации по противодействию коррупции 23 декабря 2010 г. (протокол № 21) // <https://rosmintrud.ru/ministry/programms/anticorruption/9/3>

Яшков С.А.

Современная преступность в сфере компьютерной информации: уголовно-правовой и криминологический аспект

*ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации
(Россия, Екатеринбург)*

doi: 10.18411/sr-10-06-2020-49

idsp: sciencerussia-10-06-2020-49

Аннотация

В статье предпринята попытка проанализировать состояние преступности в сфере компьютерной информации, а также обратить внимание на возможные сложности с квалификацией преступлений, предусмотренных гл. 28 УК РФ.

Ключевые слова: преступление, состав преступления, уголовная ответственность, последствия, компьютерная информация.

Главой 28 действующего Уголовного кодекса Российской Федерации (далее – УК РФ) предусмотрена ответственность за совершение преступлений в сфере компьютерной информации.

С момента принятия данного нормативного акта в 1996г. [1] и вступления его в силу с 01.01.1997г. [2] преступлениями в этой сфере считались деяния, связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием или распространением вредоносных компьютерных программ (ст. 273 УК РФ), а также нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

В 2017г. в УК РФ были внесены изменения [3], согласно которым с 01.01.2018г. среди преступлений в сфере компьютерной информации появилось еще одно – неправомерное воздействие на критическую информационную структуру Российской Федерации (ст. 274.1 УК РФ).

О распространенности преступности в сфере компьютерной информации можно судить по правоприменительной практике.

Так, согласно статистическим данным, изложенным на официальном сайте Министерства внутренних дел Российской Федерации [4], за 2019г. в России было зарегистрировано 2 883 преступления в сфере компьютерной информации, из которых 2 420 связаны с неправомерным доступом к компьютерной информации (ст. 272 УК РФ) и 455 – созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ). Нетрудно посчитать, что на состав преступления, предусмотренный ст. 274 УК РФ, приходится 8 преступлений.

В данную статистику не вошли преступления, предусмотренные ст. 274.1 УК РФ, поскольку согласно ст. 151 Уголовно-процессуального кодекса Российской Федерации расследование данного состава преступления относится к ведению органов Федеральной службы безопасности Российской Федерации. Поэтому статистические данные по ст. 274.1 УК РФ не могут находиться на официальном сайте МВД России, а на сайте ФСБ России они не были найдены.

Судебная практика применения данных составов преступлений в настоящее время выглядит следующим образом.

На сайте Государственной автоматизированной системы Российской Федерации «Правосудие» (ГАС РФ «Правосудие») [5], рекомендованной Верховным Судом Российской Федерации к внедрению в федеральных судах общей юрисдикции [6], есть информация о 70 вынесенных в 2019г. приговорах по уголовным делам по ст. 272 УК РФ (13 – по ч. 1, 17 – по ч. 2 и 40 – по ч. 3), 53 – по ст. 273 УК РФ (24 – по ч. 1 и 29 – по ч. 2) и 2 по ст. 274 УК РФ (оба по ч. 1).

Сведения о применении ст. 274.1 УК РФ достаточно скудны. Так, в указанной автоматизированной системе имеется информация всего о двух прекращенных в 2019г. уголовных делах по ч. 1 ст. 274.1 УК РФ (одно – в связи с назначением судебного штрафа, второе – в связи деятельным раскаянием) и двух вынесенных за этот же период приговорах (по ч. 4 ст. 274.1 УК РФ).

Как видно, статистика официально зарегистрированных преступлений в сфере компьютерной информации (в данном случае в расчет не берутся латентные преступления) и вынесенных приговоров разнится. Правда, в данном исследовании для сравнения приведены только вынесенные судами приговоры. Иные акты, например, судебные постановления о прекращении уголовного дела, другие, не приняты во внимание. Однако цифры говорят сами за себя – интерес криминального сообщества к совершению преступлений в сфере компьютерной информации достаточно высок.

В связи с этим следует обратить внимание не только на криминологическую характеристику преступности в названной сфере, но на возможные проблемы с квалификацией преступлений, предусмотренных гл. 28 УК РФ.

Среди всей совокупности преступных деяний, отраженных в данной главе, озабоченность вызывают 2 состава преступления – ст. 272 УК РФ и ч. 2 ст. 274.1 УК РФ, предусматривающих уголовную ответственность за неправомерный доступ к компьютерной информации.

По объективной стороне указанные составы преступления сформулированы как материальные. Это означает, что уголовно наказуемыми действия субъекта будут только в том случае, если наступят последствия, указанные в законе – уничтожение, блокирование, модификация либо копирование компьютерной информации (ч. 1 ст. 272 УК РФ) или причинение вреда критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 274.1 УК РФ).

В последнем случае законодатель не уточняет, что из себя могут представлять последствия, обозначенные им как «вред». Очевидно, в данном случае можно говорить о любом вреде, в том числе уничтожении, блокировании, модификации и копировании информации, содержащейся в критической информационной инфраструктуре Российской Федерации. Данный вывод сделан исходя из способа совершения преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, – использование компьютерных программ, иной компьютерной информации или вредоносных компьютерных программ.

Анализируя объективную сторону составов указанных преступлений, а, именно, действие, выраженное в «неправомерном доступе к охраняемой компьютерной информации», следует прийти к неоднозначному выводу о том, будет ли наступать

уголовная ответственность за осуществление неправомерного доступа, который не повлек последствий, указанных в ст. 272 УК РФ и ч. 2 ст. 274.1 УК РФ.

Так, механизм действия злоумышленника, выраженный в «неправомерном доступе к компьютерной информации» можно рассматривать и как процесс (сами действия, направленные на доступ к компьютерной информации), и как состояние (последствие действий, связанных с доступом к компьютерной информации).

Совершенно очевидно, что в случае совершения «процедурных» действий, направленных на неправомерный доступ к охраняемой компьютерной информации, может быть причинен вред, указанный в законе. Тем более, если эти действия будут совершены, например, с использованием вредоносных компьютерных программ (как это прямо указано в ч. 2 ст. 274.1 УК РФ). Тогда состав преступления будет иметь место.

Если же в процессе этих действий не последовали последствия, можно ли говорить о составе преступления? В этом случае речь идет о том, как квалифицировать действия, когда имел место неправомерный доступ к охраняемой компьютерной информации, но те последствия, которые указаны в законе – «уничтожение, блокирование, модификация либо копирование компьютерной информации» (ч. 1 ст. 272 УК РФ) или «причинение вреда критической информационной инфраструктуре Российской Федерации» (ч. 2 ст. 274.1 УК РФ), – не наступили.

Так, в настоящее время хакеры с использованием компьютерных средств, программного обеспечения могут получить доступ к совершенно различной информации. Например, «взломав» какой-либо сайт или информационно-телекоммуникационную сеть и отыскав интересующую информацию, они могут остановиться на этом, и не совершать никаких действий, направленных на уничтожение, блокирование, модификацию либо копирование компьютерной информации или причинение вреда критической информационной инфраструктуре Российской Федерации.

В этом заключается доступ к охраняемой компьютерной информации как результат действий, когда с информацией лицо ознакомилось, а последствий, указанных в законе, нет.

Нельзя утверждать, что в данном случае наступили какие-либо последствия вообще, тем более те, что указаны в ст. 272 УК РФ и ч. 2 ст. 274.1 УК РФ.

Так, уничтожения, блокирования или модификации действительно не имеет место.

Возможно, есть необходимость обсудить вопрос – нельзя ли в качестве наступившего вреда в данном случае рассматривать копирование информации, поскольку злоумышленником она была, как минимум, прочитана. Не скопировал ли он ее?

Думается, что вопрос о «копировании» как об объективной стороне состава преступления здесь сложен и неоднозначен.

Дело в том, что процесс копирования можно представить как копирование файла, с одной стороны, и копирование информации, с другой.

Копирование файла – это создание его копии, содержащей информацию. Копирование имеет место при переносе файлов на какой-либо носитель (например, флэшку, оптический диск, внешний жесткий диск).

Отсюда следует, что под копированием с данной точки зрения можно понимать лишь умышленные действия по созданию копии файла на каком-либо носителе. Таким образом, «ознакомление» с информацией с экрана монитора нельзя рассматривать как копирование файла.

Копирование информации представляет собой создание копии какой-либо информации. Любая копия информации предполагает стопроцентную идентичность оригиналу. Следовательно, считывание информации с экрана монитора также не может признаваться копированием информации, поскольку в большинстве случаев мозг человека не сможет запомнить и потом воспроизвести в зеркальном отражении все то, что было на экране монитора.

Так, например, если на экране монитора открыта программа с какой-либо базой данных, в которой большое количество ячеек, имеющих собственное название, а в этих ячейках зафиксировано множество наименований продукции и ее стоимость, то запомнить даже одну страничку этой базы для среднестатистического человека будет невозможным.

Таким образом, исходя из понятия компьютерной информации, данном в примечании к ст. 272 УК РФ, согласно которому под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, можно сделать вывод, что копирование компьютерной информации следует понимать в узком смысле этого слова, то есть копирование файла, содержащего информацию.

Отсюда следует, что неправомерные действия, связанные с доступом к охраняемой компьютерной информации, в том числе содержащейся в критической информационной инфраструктуре Российской Федерации, с целью ее ознакомления в настоящее время по российскому уголовному законодательству не наказуемы.

Нельзя признать данные действия также покушением, поскольку, как сказано выше, неправомерный доступ следует рассматривать и как процедуру, и как состояние. И в том, и в другом случае действие уже было совершено. А когда у злоумышленника нет целей достижения последствий, указанных в ст. 272 УК РФ или ч. 2 ст. 274.1 УК РФ, такие действия вряд ли можно назвать даже оконченным покушением.

В связи с вышеизложенным следует отметить, что в настоящее время могут иметь место проблемы с квалификацией действий виновных по ст. 272 УК РФ и ч. 2 ст. 274.1 УК РФ, если они не повлекли за собой последствий, указанных в законе.

При наличии к тому оснований можно подумать об уголовно-правовой оценке действий виновных не по нормам гл. 28 «Преступления в сфере компьютерной информации», а по нормам гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» или гл. 22 «Преступления в сфере экономической деятельности».

1. Уголовный кодекс Российской Федерации от 13.06.1996г. № 63-ФЗ // Российская газета. 1996. 18-20, 25 июня.
2. Федеральный закон от 13.06.1996г. № 64-ФЗ «О введении в действие Уголовного кодекса Российской Федерации» // Российская газета. 1996. 18 июня.
3. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 194-ФЗ // Российская газета. 2017. 31 июля.
4. <https://мвд.рф> (дата обращения – 04.06.2020г.)
5. <https://sudrf.ru/> (дата обращения – 04.06.2020г.)
6. Постановление Совета судей Российской Федерации от 30.11.2006г. № 170 об утверждении акта Государственной комиссии по приемке работ по созданию системных и программно-технических решений ГАС «Правосудие» // Судебный департамент при Верховном Суде Российской Федерации / <http://www.cdep.ru/index.php?id=256> (дата обращения – 04.06.2020г.).